НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200401.4 | 1 апреля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ПО LibreOffice

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	LibreOffice до v6.2.6
Дата выявления	31 марта 2017 г.
Дата обновления	1 апреля 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2019-9848	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного документа, содержащего вредоносный код на языке Python. Уязвимость обусловлена некорректной проверкой входных данных в компоненте LibreLogo. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-94: Некорректное управление генерированием кода (внедрение кода) Рекомендации по устранению: обновить программное обеспечение.	8,8

MITRE: CVE-2019-9850	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного документа, содержащего вредоносный код на языке Python. Уязвимость обусловлена некорректной проверкой URL-адреса, позволяя выполнять сценарии в компоненте LibreLogo. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	9,8
MITRE: CVE-2019-9851	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством открытия пользователем специально созданного вредоносного документа. Уязвимость обусловлена некорректной обработкой сценариев LibreLogo. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	8,8
MITRE: CVE-2019-9852	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством открытия пользователем специально созданного вредоносного документа. Уязвимость обусловлена некорректным кодированием URL-адреса при проверке местоположения скрипта. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога) Рекомендации по устранению: обновить программное обеспечение.	8,8

MITRE: CVE-2019-9853	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с привилегиями текущего пользователя в целевой системе посредством открытия пользователем специально созданного вредоносного документа. Уязвимость обусловлена некорректной проверкой входных данных при декодировании URL-адреса в расположении макроса. CVSSv3.0: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	8,0
MITRE: CVE-2019-9854	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код с привилегиями текущего пользователя в целевой системе посредством открытия пользователем специально созданного вредоносного документа. Уязвимость обусловлена некорректной обработкой URL-адреса сценария. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: обновить программное обеспечение.	9,8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020040104 https://nvd.nist.gov/vuln/detail/CVE-2019-9848 https://nvd.nist.gov/vuln/detail/CVE-2019-9850 https://nvd.nist.gov/vuln/detail/CVE-2019-9851 https://nvd.nist.gov/vuln/detail/CVE-2019-9852 https://nvd.nist.gov/vuln/detail/CVE-2019-9853 https://nvd.nist.gov/vuln/detail/CVE-2019-9854 https://access.redhat.com/errata/RHSA-2020:1151